SecurityMetrics

GUIDED HIPAA COMPLIANCE

HIPAA SOLUTIONS FOR OFFICE MANAGERS AND PRACTITIONERS

securityMETRICS®

GUIDED HIPAA COMPLIANCE OVERVIEW

Our objective is to make life easier for office managers and practitioners. The SecurityMetrics HIPAA Dashboard helps you keep compliance efforts organized and progressing. You can track your breach protection status, risk management plan, training, and policies and procedures all in one place. We guide you through HIPAA compliance in three steps:

- Breach Protection Consulting
- Guided Risk Analysis
- Prioritized Risk Management Plan Implementation

1 BREACH PROTECTION CONSULTING

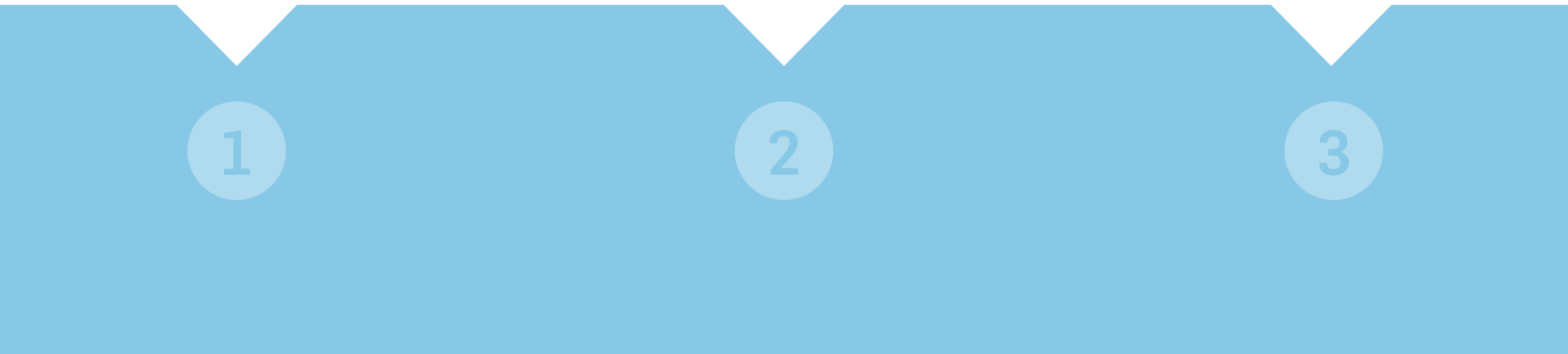
Increase data security in your organization to prevent a breach

2 GUIDED RISK ANALYSIS

Understand your organization's vulnerabilities

3 PRIORITIZED RISK MANAGEMENT PLAN

Implement your organization's prioritized plan



1 2 3

BREACH PROTECTION CONSULTING

We help you protect your organization from breach and fines

HIPAA BREACH PROTECTION CHECKLIST

A SecurityMetrics HIPAA Support Advisor analyzes the top risks to your organization's data, which include: password management, firewalls, malware, remote access, wireless security, web browsing, email, theft, and social engineering. Addressing vulnerabilities found during the top risks review significantly increases your organization's data security.

HIPAA BREACH PROTECTION

We are so confident in our ability to help you secure your systems that we back our services with $100,000 breach protection. In the event of a compromise, this assists you with costs associated with regulatory fines and penalties associated with HIPAA violations and forensic investigations.

MONTHLY RESOURCES

SecurityMetrics provides a monthly newsletter that covers HIPAA compliance and management tips, educational materials, and recent healthcare news. These resources help you stay updated, knowledgeable, and avoid pitfalls that lead to data compromise.

1 2 3

GUIDED RISK ANALYSIS

We do the heavy lifting of the risk analysis

HIPAA COMPLIANCE RISK ANALYSIS

Health and Human Services (HHS) has levied fines for the lack of a formal and thorough risk analysis. SecurityMetrics provides an analysis of your current compliance level, a map of all systems that interact with PHI, and vulnerability and risk identification. SecurityMetrics Guided Risk Analysis includes our award-winning support to ensure your risk analysis is accurate and complete.

SYSTEM VULNERABILITY IDENTIFICATION

All systems used to create, receive, maintain, and transmit PHI have inherent risks. As data security experts, SecurityMetrics identifies risks and vulnerabilities based on your systems in use. After creating a PHI map of your systems that interact with PHI, we produce a list of associated risks, threats, and vulnerabilities.

EXTERNAL NETWORK VULNERABILITY SCANS

Data thieves access protected health information (PHI) through unprotected networks. Our vulnerability scans help you achieve external network security by searching for even the most recent vulnerabilities. Our finely tuned scan engines expose weaknesses in your network. Our support team helps you repair discovered vulnerabilities to protect your patient data.

PRIORITIZED RISK MANAGEMENT

After performing the risk analysis, SecurityMetrics provides a prioritized risk management plan. This plan is based on the results from your organization's systems, controls, risks, and vulnerabilities. The risk management plan is prioritized from high to low risk to address the most threatening risks first.

"I appreciated the expert help from SecurityMetrics as our office worked through understanding HIPAA regulations. The staff was knowledgeable and very helpful. The validation process went off without a hitch!"

– Kathy Marks,
Office of Dr. Mike Bloom

PRIORITIZED RISK MANAGEMENT PLAN IMPLEMENTATION

We get you secure and HIPAA compliant

GUIDED RISK MANAGEMENT PLAN IMPLEMENTATION

Understanding the technical action items in the risk management plan can be difficult. SecurityMetrics HIPAA experts guide you and your IT resources through implementation to ensure your organization is secure and compliant.

POLICIES AND PROCEDURES

HIPAA policies and procedures aren't just paperwork—they are the blueprint to your organization's daily compliance efforts. SecurityMetrics provides customizable Privacy Rule (29), Security Rule (16), and Breach Notification policies and related procedures. SecurityMetrics' policies and procedures templates save you time, energy, and money so you can focus on managing your organization. An assigned support specialist assists you in tailoring policies and procedures so that they accurately reflect the uniqueness of your organization.

ADDITIONAL SECURITY AND COMPLIANCE TOOLS

SecurityMetrics has additional tools to help you secure PHI and reach full HIPAA compliance. We offer data security and HIPAA training, penetration testing, onsite compliance assessments, and HIPAA consulting to meet your organizations unique needs.

COMPLIANCE CERTIFICATE

Once you complete your risk management plan implementation, SecurityMetrics provides a compliance certificate. The certificate verifies your compliance, assures your patients that you care about and protect their data, and is suitable for prominent display in your office.

GUIDED HIPAA COMPLIANCE PACKAGES

PRO	PLUS	BASIC
$4999	*$2499*	*$999*
Online Portal Access (for real-time HIPAA guidance, logging, storage, documentation, and training)	Online Portal Access (for real-time HIPAA guidance, logging, storage, documentation, and training)	Online Portal Access (for real-time HIPAA guidance, logging, storage, documentation, and training)
Breach Protection Checklist	Breach Protection Checklist	Breach Protection Checklist
$100,000 Service Guarantee (After attesting to Breach Protection Checklist)	$100,000 Service Guarantee (After attesting to Breach Protection Checklist)	$100,000 Service Guarantee (After attesting to Breach Protection Checklist)
Risk Analysis	Risk Analysis	Risk Analysis
Risk Management Plan	Risk Management Plan	Risk Management Plan
HIPAA Policies & Procedures (including Breach Notification Policy & Business Associate Agreement Template)	HIPAA Policies & Procedures (including Breach Notification Policy & Business Associate Agreement Template)	HIPAA Policies & Procedures (including Breach Notification Policy & Business Associate Agreement Template)
Dedicated HIPAA Coach to guide you through Risk Analysis & Risk Management Plan	**Monthly Vulnerability Scans (3 IP addresses)**	Monthly Vulnerability Scans (1 IP address)
Monthly Vulnerability Scans (5 IP addresses)	**HIPAA Training (9 Seats)**	
HIPAA Training (25 Seats)	**Dedicated HIPAA Coach to guide you through Risk Analysis & Risk Management Plan**	
Up to 4 hours with a HIPAA Specialist for deeper discovery and a start to remediation of high risk areas		

ADDITIONAL PRODUCTS AND SERVICES

Managed Firewall	Penetration Testing
Onsite HIPAA Assessment	Forensic Investigation

All SecurityMetrics HIPAA Compliance packages are an annual subscription that will be automatically renewed.

HIPAA COMPLIANCE FAQ

WHAT IS THE PURPOSE OF HIPAA?

The use of electronic health records has the potential to reduce costs and improve care, but has caused an increased focus on data security and introduced new vulnerabilities to healthcare organizations. The Health Insurance Portability and Accountability Act (HIPAA) was enacted to protect patient information. HIPAA includes rules on privacy, security, and breach notification with regard to protecting consumer healthcare information.

WHO ENFORCES HIPAA?

HIPAA is regulated and enforced by the Health and Human Services (HHS) Office for Civil Rights (OCR). Recent changes to HIPAA legislation have provided additional guidance and authority for the OCR to enforce HIPAA compliance through audits and financial penalties. The State Attorney General has been given authority to also levy fines related to HIPAA violations and compromises.

HOW MUCH CAN I BE FINED?

The penalties outlined below are assessed per day and per violation.

VIOLATION CATEGORY	PENALTY	MAXIMUM/CALENDAR YEAR
(A) Did not know	$100-$50,000	$1,500,000
(B) Reasonable Cause	$1,000-$50,000	$1,500,000
(C) (i) Willful Neglect-Corrected	$10,000-$50,000	$1,500,000
(C) (ii)Willful Neglect-Not Corrected	$50,000	$1,500,000

After a breach, the HHS is not the only one with authority to mandate fines. We are also seeing class action lawsuits, State Attorney Generals, and the FTC collecting money based on HIPAA violations.

WHY THE INCREASED ENFORCEMENT?

Over 147 million breached patient records have been reported to the HHS since 2009. These breached records have negatively impacted covered entities and business associates, resulting in over $41 million in resolution agreements and fines.

WHAT TRAININGS AM I REQUIRED TO DO?

HIPAA requires regular employee training on both the Privacy and Security Rules. Other trainings you may consider include data security, responsible use of social media, and Payment Card Industry Data Security Standard (PCI DSS). SecurityMetrics provides these trainings.

IS THERE A WAY TO TEST MY ORGANIZATION'S RISK OF BREACH?

Penetration testing, or ethical hacking, is the most accurate way to know your data is safe. A penetration test analyst examines your business environment and manually checks your network to find weaknesses the way a hacker would, through live testing. SecurityMetrics Penetration Test Analysts are experts at helping protect sensitive data.

AM I REQUIRED TO HAVE AN ONSITE ASSESSMENT?

Onsite assessments conducted by a third party are not required to achieve HIPAA compliance, but in many cases they are recommended. Depending on the complexity of your IT infrastructure, the number of locations you have, and the way you work with PHI, you may want to consider an onsite assessment. For the majority of small covered entities, an offsite HIPAA compliance assessment is sufficient to reach compliance with the law.

HOW DO I BECOME HIPAA COMPLIANT?

Most offices have made some progress towards HIPAA compliance. However, with recent changes and an increased focus on technical security, offices are falling short. Both Privacy and Security Rules require covered entities and business associates to:

- Conduct an acceptable risk analysis
- Prepare an actionable risk management plan
- Make regular and demonstrable progress on the plan

SECURITYMETRICS

Secure Data. Report Compliance.

Since its founding in 2000, privately-held SecurityMetrics has grown from a small security company specializing in vulnerability assessment scans to a global leader of data security and compliance solutions. Headquartered in Orem, Utah, SecurityMetrics continues to provide expert security and compliance services needed to protect organizations around the world.

OUR MISSION

We aim to help organizations comply with mandates through innovative security tools, friendly customer support, and qualified expertise.

OUR EXPERTISE

We have more than 15 years of experience with data security and compliance, and have helped over 800,000 customers. Our employees hold certifications like:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Qualified Security Assessor (QSA)
- Approved Scanning Vendor (ASV)
- Healthcare Information Security and Privacy Practitioner (HCISPP)

TO DISCUSS YOUR OFFICE'S HIPAA SITUATION, CONTACT US.

877.364.9183

hipaa@securitymetrics.com

securityMETRICS®